

ENKRIPSI CITRA DIGITAL MEDIS MENGGUNAKAN ALGORITMA ELLIPTIC CURVE CRYPTOGRAPHY

Diajukan Sebagai Syarat Untuk Menyelesaikan
Pendidikan Program Strata-1 Pada
Jurusan Teknik Informatika



Oleh :
Kintan Semi Melinda
NIM : 09021181520133

**Jurusan Teknik Informatika
FAKULTAS ILMU KOMPUTER UNIVERSITAS
SRIWIJAYA
2020**

LEMBAR PENGESAHAN SKRIPSI

ENKRIPSI CITRA DIGITAL MEDIS MENGGUNAKAN
ALGORITMA *ELLIPTIC CURVE CRYPTOSYSTEM (ECC)*

Oleh :

Kintan Semi Melinda
NIM : 09021181520133

Indralaya, 2020

Pembimbing I,


Drs. Megah Mulya, M.T.
NIP. 1966022020060410001

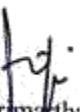
Pembimbing II,


Osvari Arsalan, M.T.
NIP. 1988062820180310001

Mengetahui,

Ketua Jurusan Teknik Informatika




Riskie Primaatha, M.T.
NIP.197706012009121004

TANDA LULUS UJIAN SIDANG SKRIPSI

Pada hari telah dilaksanakan ujian sidang skripsi oleh Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.

Nama : Kintan Semi Melinda
NIM : 09021181520133
Judul : Enkripsi Citra Digital Medis Menggunakan Algoritma *Elliptic Curve Cryptosystem*.

1. Pembimbing I

Drs. Megah Mulya, M.T
NIP. 196602202006041001

2. Pembimbing II

Osvari Arsalan, M.T
NIP. 198806282018031001

3. Pengaji I

Samsuryadi, M.Kom., Ph.D.
NIP. 197102041997021003

4. Pengaji II

Mastura Diana Marieska, M.T.
NIP. 198603212018032001

Mengetahui,

Ketua Jurusan Teknik Informatika



Rifkie Primartha S.T. M.T.
NIP 197706012009121004

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama : Kintan Semi Melinda
NIM : 09021181520133
Program Studi : Teknik Informatika
Judul : Enkripsi Citra Digital Medis Menggunakan Algoritma *Elliptic Curve Cryptosystem.*

Hasil Pengecekan Software *iThenticate/Turnitin* : 15 %

Menyatakan bahwa Laporan Projek saya merupakan hasil karya sendiri dan bukan hasil penjiplakan/plagiat. Apabila ditemukan unsur penjiplakan/plagiat dalam laporan projek ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian, pernyataan ini saya buat dengan sebenarnya dan tidak ada paksaan oleh siapapun.

Indralaya, 2020



Kintan Semi Melinda
NIM. 09021181520133

Motto :

- As long as there's life, there's hope. Just keep moving forward.

Kupersembahkan karya tulis ini

kepada :

- Allah SWT
- Kedua Orang Tuaku
- My Family
- Sahabat dan teman seperjuanganku
- Keluarga Besar Teknik Informatika Universitas Sriwijaya
- Almamaterku

KATA PENGANTAR



Alhamdulillah, puji dan syukur kehadirat Allah SWT atas segala nikmat, rahmat, dan karunia-Nya, sehingga penulis dapat menyelesaikan tugas akhir dengan baik. Tugas akhir ini disusun untuk memenuhi salah satu syarat guna menyelesaikan pendidikan program Strata-1 pada Fakultas Ilmu Komputer Program Studi Teknik Informatika di Universitas Sriwijaya.

Untuk selanjutnya penyusun mengucapkan banyak terima kasih kepada pihak-pihak yang telah membantu dalam penyelesaian skripsi ini, yaitu :

1. Pemerintah DIKTI dan Universitas Sriwijaya yang telah memberikan kesempatan dan berbagai fasilitas dalam perkuliahan sehingga saya dapat menyelesaikan tugas akhir ini;
2. Orang Tuaku tercinta Bapak Jhon Davidson dan Ibu Laily Hayati, serta seluruh keluarga besarku yang selalu memberikan dukungan berharga berupa kasih saying, didikan, nasihat, motivasi dan doa.
3. Bapak Jaidan Jauhari, S.Pd., M.T. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya;
4. Bapak Rifkie Primartha, M.T. selaku ketua Jurusan Teknik Informatika Universitas Sriwijaya;
5. Bapak Rusdi Efendi, M.Kom. selaku pembimbing akademik yang telah memberikan saran dan kritik kepada penulis selama masa perkuliahan;
6. Bapak Drs. Megah Mulya, M.T dan Osvari Arsalan, S.Kom., M.T selaku pembimbing tugas akhir yang telah bersedia meluangkan waktu untuk

memberikan bimbingan dan ilmu pengetahuan untuk menyelesaikan tugas akhir ini;

7. Bapak Samsuryadi, M.Kom., Ph.D._dan Mastura Diana Marieska, M.T. selaku penguji yang telah memberikan tanggapan, kritik, saran dan nasehat untuk menyelesaikan tugas akhir ini dengan baik;
8. Seluruh Bapak dan Ibu Dosen Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya yang telah memberikan ilmu pengetahuan kepada penulis selama kegiatan akademik berlangsung;
9. Kak Ricy serta seluruh staf tata usaha yang telah membantu dalam kelancaran proses administrasi dan akademik selama masa perkuliahan;
10. Teman – teman gibah pagi yang telah memberikan dukungan dan bantuan kepada penulis;
11. Yamazaki Kento, Ken Kaneki, Kirigaya Kazuto, Eren Yeager, Roronoa Zoro, Ranpo Edogawa, Ciel Phantomhive, dan Mereoleona Vermillion yang telah memotivasi penulis dalam penulisan tugas akhir ini.
12. Achma Desvania dan Wiliyanti sebagai sahabat berdiskusi dan saling mendukung dalam penulisan tugas akhir ini.

Inderalaya, 2020

Penulis,

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN LEMBAR PENGESAHAN.....	ii
HALAMAN PERSETUJUAN KOMISI PENGUJI.....	iii
HALAMAN PERNYATAAN.....	iv
HALAMAN MOTTO DAN PERSEMBAHAN.....	v
ABSTRACT.....	vi
ABSTRAK.....	vii
KATA PENGANTAR.....	viii
DAFTAR ISI.....	x
DAFTAR TABEL.....	xii
DAFTAR GAMBAR	xiv
DAFTAR LAMPIRAN.....	xv

BAB I PENDAHULUAN

1.1 Pendahuluan.....	I-1
1.2 Latar Belakang Masalah.....	I-1
1.3 Rumusan Masalah.....	I-2
1.4 Tujuan Penelitian.....	I-2
1.5 Manfaat Penelitian.....	I-3
1.6 Batasan Masalah.....	I-3
1.7 Sistematika Penulisan.....	I-4
1.8 Kesimpulan.....	I-5

BAB II KAJIAN LITERATUR

2.1 Pendahuluan.....	II-1
2.2 Kriptografi.....	II-1
2.2.1 Algoritma Simetris.....	II-2
2.2.2 Algoritma Asimetris.....	II-2
2.3 Citra.....	II-4
2.3.1 Enkripsi Citra.....	II-4
2.4 Digitalisasi Sampling.....	II-5
2.4.1 <i>Diffie-Hellman Key Exchange Algorithm</i>	II-6
2.5 <i>Elliptic Curve Cryptography</i>	II-7
2.5.1 Kurva Eliptik Pada Himpunan Fp.....	II-8
2.6 Domain Parameter Kurva Eliptik.....	II-10
2.7 Pengukuran Kualitas Enkripsi.....	II-11
2.7.1 Hitogram.....	II-12
2.8 <i>Rational Unified Process (RUP)</i>	II-13
2.9 Penelitian yang Relevan.....	II-14
2.10 Kesimpulan.....	II-18

BAB III METODOLOGI PENELITIAN

3.1	Pendahuluan.....	III-1
3.2	Pengumpulan Data.....	III-1
3.2.1	Jenis Data.....	III-1
3.2.2	Sumber Data.....	III-1
3.2.3	Metode Pengumpulan Data.....	III-1
3.3	Tahap Penelitian.....	III-2
3.3.1	Menetapkan Kerangka Kerja.....	III-3
3.3.1.1	Kerangka Kerja Proses Enkripsi.....	III-3
3.3.1.2	Kerangka Kerja Proses Dekripsi.....	III-4
3.3.1	Menetapkan Kriteria Pengujian.....	III-4
3.3.2	Menetapkan Format Data Pengujian.....	III-5
3.3.3	Menentukan Alat Yang Digunakan Dalam Pelaksanaan Penelitian.	III-5
3.3.4	Melakukan Pengujian Penelitian	III-6
3.3.5	Melakukan Analisa Hasil dan Membuat Kesimpulan Penelitian....	III-6
3.4	Metode Pengembangan Perangkat Lunak.....	III-7
3.4.1	Fase Insepsi	III-8
3.4.2	Fase Elaborasi.....	III-8
3.4.3	Fase Konstruksi.....	III-9
3.4.4	Fase Transisi.....	III-10
3.5	Manajemen Proyek Penelitian.....	III-10

BAB IV PENGEMBANGAN PERANGKAT LUNAK

4.1	Pendahuluan.....	IV-1
4.2	Fase Insepsi.....	IV-1
4.2.1	Pemodelan Bisnis.....	IV-1
4.2.2	Kebutuhan Sistem.....	IV-2
4.2.2.1	Fitur Enkripsi-Dekripsi.....	IV-2
4.2.2.2	Fitur Menampilkan Histogram.....	IV-2
4.2.3	Analisis Design.....	IV-4
4.2.3.1	Analisis Kebutuhan Perangkat Lunak.....	IV-4
4.2.3.2	Analisis Data.....	IV-4
4.2.3.3	Analisis Fitur Enkripsi.....	IV-5
4.2.3.4	Analisis Fitur Dekripsi.....	IV-5
4.2.3.5	Desain Perangkat Lunak.....	IV-5
4.3	Fase Elaborasi.....	IV-15
4.3.1	Pemodelan Bisnis.....	IV-15
4.3.1.1	Perancangan Data.....	IV-15
4.3.1.2	Perancangan Antarmuka.....	IV-16
4.3.2	Kebutuhan Sistem.....	IV-17
4.3.3	Digram Sequence.....	IV-17
4.4	Fase Konstruksi.....	IV-19
4.4.1	Kebutuhan Sistem.....	IV-19
4.4.2	Diagram Kelas.....	IV-20
4.4.3	Implementasi.....	IV-21
4.4.4.1	Implementasi Kelas.....	IV-21
4.4.4.2	Implementasi Antarmuka.....	IV-21

4.5	Fase Transisi.....	IV-23
4.5.1	Pemodelan Bisnis.....	IV-23
4.5.2	Kebutuhan Sistem.....	IV-24
4.5.3	Rencana Pengujian.....	IV-24
4.5.3.1	Rencana Pengujian <i>Use Case</i> Enkripsi Citra.....	IV-24
4.5.3.2	Rencana Pengujian <i>Use Case</i> Dekripsi Citra.....	IV-25
4.5.3.3	Rencana Pengujian <i>Use Case</i> Melihat.....	IV-25
	Histogram Citra Asli.....	IV-26
4.5.3.4	Rencana Pengujian <i>Use Case</i> Melihat Histogram Citra Enkripsi.....	IV-26
4.5.4	Implementasi.....	IV-26
4.5.4.1	Pengujian <i>Use Case</i> Enkripsi.....	IV-27
4.5.4.1	Pengujian <i>Use Case</i> Dekripsi.....	IV-29
4.5.4.1	Pengujian <i>Use Case</i> Melihat Histogram Citra Asli.....	IV-30
4.5.4.1	Pengujian <i>Use Case</i> Melihat Histogram Citra Enkripsi....	IV-32
4.6	Kesimpulan.....	IV-35

BAB V HASIL DAN ANALISIS PENELITIAN

5.1	Pendahuluan.....	V-1
5.2	Data Hasil Percobaan/Penelitian.....	V-1
5.2.1	Konfigurasi Penelitian.....	V-1
5.2.2	Data Hasil Konfigurasi.....	V-1
	5.2.2.1 Hasil Enkripsi <i>Elliptic Curve</i> Pada Citra Medis dan Hasil Pengujian Histogram.....	V-2
5.3	Analisis Hasil Pengujian Histogram.....	V-4
5.4	Kesimpulan.....	V-4

BAB VI KESIMPULAN DAN SARAN

6.1	Kesimpulan.....	VI-1
6.2	Saran.....	VI-1

DAFTAR PUSTAKA.....	ix
---------------------	----

DAFTAR TABEL

Tabel II-1.	Hasil Analisis Pengujian Entropy Enkripsi dan Dekripsi Citra Digital Medis Menggunakan Algoritma Kurva Eliptik	II-5
Tabel II-2.	Hasil Analisis Pengujian Waktu Eksekusi Enkripsi dan Dekripsi Citra Digital Menggunakan Algoritma Kurva Eliptik ...	II-15
Tabel II-3.	Image Encryption Time Using Elliptic Curve Cryptography	II-16
Tabel II-4.	Waktu Eksekusi Enkripsi dan Dekripsi Citra Digital Medis Menggunakan Improvisasi Algoritma Elgamal	II-18
Tabel III-1.	Hasil Pengujian Histogram Citra	III-5
Tabel III-2.	Penjadwalan Penelitian dalam Bentuk <i>Work Breakdown Structure</i> (WBS)	III-11
Tabel IV-1.	Kebutuhan Fungsional	IV-3
Tabel IV-2.	Kebutuhan Non-Fungsional	IV-3
Tabel IV-3.	Definisi Aktor	IV-6
Tabel IV-4.	Defnisi <i>Use Case</i>	IV-6
Tabel IV-5.	Skenario <i>Use Case</i> Enkripsi Citra	IV-8
Tabel IV-6.	Skenario <i>Use Case</i> Dekripsi Citra	IV-9
Tabel IV-7.	Skenario <i>Use Case</i> Melihat Histogram Citra Asli	IV-10
Tabel IV-8.	Skenario <i>Use Case</i> Melihat Histogram Citra Enkripsi	IV-11
Tabel IV-9.	Implementasi Kelas	IV-21
Tabel IV-10.	Rencana Pengujian <i>Use Case</i> Enkripsi Citra	IV-24
Tabel IV-11.	Rencana Pengujian <i>Use Case</i> Dekripsi Citra	IV-25
Tabel IV-12.	Rencana Pengujian <i>Use Case</i> Melihat Histogram Citra Asli	IV-25
Tabel IV-13.	Rencana Pengujian <i>Use Case</i> Melihat Histogram Citra Enkripsi	IV-26
Tabel IV-14.	Pengujian <i>Use Case</i> Enkripsi	IV-27
Tabel IV-15.	Pengujian <i>Use Case</i> Dekripsi	IV-29
Tabel IV-16.	Pengujian <i>Use Case</i> Melihat Histogram Citra Asli	IV-31
Tabel IV-17.	Pengujian <i>Use Case</i> Melihat Histogram Citra Enkripsi	IV-32
Tabel V-1.	Hasil Enkripsi <i>Elliptic Curve</i> Pada Citra Medis dan Hasil Pengujian Histogram	V-2

DAFTAR GAMBAR

Gambar II-1. Pertukaran Kunci Diffie-Hellman	II-6
Gambar II-2. Perbedaan Histogram Citra Asli dan Citra Enkripsi.....	II-12
Gambar II-3. Struktur Proses RUP	II-13
Gambar III-1. Diagram Tahapan Penelitian	III-2
Gambar III-2. Diagram Tahapan Proses Enkripsi	III-3
Gambar III-3. Diagram Tahapan Proses Dekripsi	III-4
Gambar III-4. Diagram Pengujian Penelitian	III-6
Gambar III-5. Penjadwalan Penelitian Tahap Menentukan Ruang Lingkup dan Unit Penelitian	III-15
Gambar III-6. Penjadwalan Penelitian Tahap Menentukan Dasar Teori yang Berkaitan dengan Penelitian	III-15
Gambar III-7. Penjadwalan Penelitian Tahap Menentukan Kriteria Pengujian	III-16
Gambar III-8. Penjadwalan Penelitian Tahap Menentukan Alat yang Digunakan Untuk Pelaksanaan Penelitian Pada Fase Insepsi .	III-16
Gambar III-9. Penjadwalan Penelitian Tahap Menentukan Alat yang Digunakan Untuk Pelaksanaan Penelitian Pada Fase Elaborasi	III-17
Gambar III-10. Penjadwalan Penelitian Tahap Menentukan Alat yang Digunakan Untuk Pelaksanaan Penelitian Pada Fase Konstruksi	III-18
Gambar III-11. Penjadwalan Penelitian Tahap Menentukan Alat yang Digunakan Untuk Pelaksanaan Penelitian Pada Fase Transisi.....	III-19
Gambar III-12 Penjadwalan Penelitian Tahap Melakukan Pengujian Penelitian	III-19
Gambar III-13. Penjadwalan Penelitian Tahap Melakukan Analisa Hasil Pengujian dan Membuat Kesimpulan	III-21
Gambar IV-1. Diagram <i>Use Case</i> Enkripsi Citra Digital Medis	IV-1
Gambar IV-2. Diagram Aktivitas Enkripsi Citra	IV-12
Gambar IV-3. Diagram Aktivitas Dekripsi Citra	IV-13
Gambar IV-4. Diagram Aktivitas Melihat Histogram Citra Asli	IV-14
Gambar IV-5. Diagram Aktivitas Melihat Histogram Citra Enkripsi	IV-14
Gambar IV-6. Rancangan Antarmuka <i>Elliptic Curve Encryption</i>	IV-16
Gambar IV-7. Diagram <i>Sequence</i> Enkripsi Citra	IV-18
Gambar IV-8. Diagram <i>Sequence</i> Dekripsi Citra	IV-19
Gambar IV-9. Diagram Kelas	IV-20
Gambar IV.10 Antarmuka <i>Elliptic Curve Encryption</i>	IV-23

DAFTAR LAMPIRAN

1. Dokumentasi *Source Code*

BAB I

PENDAHULUAN

1.1 Pendahuluan

Pada bab ini akan dibahas latar belakang masalah, rumusan masalah, tujuan penelitian, manfaat penelitian serta batasan masalah yang menjadi gambaran umum mengenai penelitian yang akan dilakukan.

Pendahuluan dimulai dengan penjelasan mengenai gambar digital medis, masalah dalam enkripsi dengan algoritma *elliptic curve* serta penelitian yang terkait.

1.2 Latar Belakang Masalah

Citra digital medis sebagai salah satu data digital dalam bentuk citra yang menyimpan informasi pasien. Citra medis memiliki piksel lebih besar dibanding citra biasa dengan risiko kerusakan data lebih besar (Akkasaligar & Biradar, 2017). Misalnya foto rontgen dengan sinar-X atau foto penyakit yang terlihat pada tubuh pasien yang diambil dengan bantuan komputer. Oleh karena itu sebelum dilakukan transmisi, citra perlu dilindungi agar informasi pasien terjaga kerahasiaan dan keamanannya.

Algoritma kriptografi yang biasa digunakan untuk mengamankan data diantaranya adalah RSA, Elgamal, DES, AES, tetapi jika menggunakan algoritma ini untuk enkripsi *digital image* termasuk gambar digital medis

akan memakan waktu lama dan konsumsi memori yang besar (Al-Najjar & Nazer, 2015). Algoritma *elliptic curve* telah diterapkan oleh Miller dan Koblitz untuk memperkenalkan *cryptosystem kunci public* (Society, 2012). Berdasarkan penelitian yang dilakukan oleh Vigila, algoritma elliptic curve menjadi pilihan yang dapat diterapkan untuk tipe data multimedia seperti *image*, *video*, dan *audio* dengan ukuran yang besar karena memiliki keamanan yang kuat dan waktu eksekusi yang effisien terhadap ukuran kunci (Vigila & Muneeswaran, 2009). Alasan algoritma elliptic curve memiliki keamanan yang kuat ditegaskan oleh Laiphrajkpam, bahwa secara eksponensial masalah logaritma diskrit elliptic curve sulit untuk dipecahkan (Singh & Singh, 2015).

Berdasarkan uraian latar belakang, dapat diambil kesimpulan bahwa data gambar digital medis membutuhkan pengamanan khusus karena memiliki informasi yang sangat penting. Dalam mengatasi masalah tersebut akan dilakukan penelitian mengenai dampak algoritma *elliptic curve* dalam enkripsi dan dekripsi dengan harapan algoritma tersebut cukup aman untuk diterapkan pada data gambar digital medis.

1.3 Rumusan Masalah

Rumusan masalah dalam penelitian ini yaitu apakah algoritma *elliptic curve* cukup aman untuk diterapkan dalam enkripsi dan dekripsi gambar digital medis.

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah membuktikan keamanan algoritma elliptic curve dengan melakukan analisis histogram untuk menggambarkan distribusi grafis dari intensitas nilai setiap piksel.

1.5 Manfaat Penelitian

Manfaat penelitian ini adalah sebagai berikut:

1. Hasil penelitian dapat digunakan sebagai bahan pertimbangan bagi dunia medis untuk menggunakan algoritma *elliptic curve* dalam mengamankan data gambar digital medis.
2. Hasil penelitian dapat digunakan sebagai referensi untuk penelitian ke depan.

1.6 Batasan Masalah

Batasan masalah dalam penelitian ini, yaitu citra yang digunakan adalah citra grayscale 24-bit berukuran 256 x 256 dan 512 x 512 yang berekstensi *.bmp.

1.7 Sistematika Penulisan

Sistematika penulisan tugas akhir ini mengikuti standar penulisan tugas akhir Fakultas Ilmu Komputer Universitas Sriwijaya yaitu sebagai berikut.

BAB I. PENDAHULUAN

Pada bab ini dijelaskan mengenai latar belakang masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, dan sistematika penulisan.

BAB II. KAJIAN LITERATUR

Pada bab ini akan dibahas dasar-dasar teori yang digunakan dalam penelitian, seperti tentang kriptografi, dasar-dasar *elliptic curve*, dan gambar digital medis. Pada akhir bab akan disertakan penelitian-penelitian lain yang relevan dengan penelitian ini.

BAB III. METODOLOGI PENELITIAN

Pada bab ini dijelaskan mengenai tahapan yang akan dilaksanakan pada penelitian. Setiap rencana tahapan penelitian dideskripsikan dengan detail dengan mengacu pada suatu kerangka kerja. Pada akhir bab, berisi perancangan manajemen proyek pada pelaksanaan penelitian.

1.8 Kesimpulan

Algoritma elliptic curve merupakan algoritma dengan perhitungan logaritma diskrit yang sulit untuk dipecahkan secara eksponensial sehingga memperkuat enkripsi pada data dengan ukuran besar seperti image. Berdasarkan uraian, pada penelitian ini akan dilakukan enkripsi dan dekripsi menggunakan algoritma elliptic curve untuk memastikan apakah algoritma elliptic curve cukup aman dalam enkripsi dan dekripsi gambar digital medis.

DAFTAR PUSTAKA

- AKKASALIGAR, P.T., & BIRADAR, S. 2017 Akkasaligar, P. T., & Biradar, S. (2017). Secure medical image encryption based on intensity level using Chao's theory and DNA cryptography. *2016 IEEE International Conference on Computational Intelligence and Computing Research, ICCIC 2016*. <https://doi.org/10.1109/ICCIC.2016.7919681>.
- Al-Najjar, & Hazem, M. (2011). Digital Image Encryption Algorithm Based on a Linear Independence Scheme and the Logistic Map. *Tehcnical College of Arar, Department of Computer*.
- Christensen, C. (2011). Review of Cryptography and Network Security: Principles and Practice, Fifth Edition. In *Cryptologia* (Vol. 35). <https://doi.org/10.1080/01611194.2010.533253>.
- Kruchten, P. (2004). The Rational Unified Process: An Introduction. In *Addison-Wesley Professional*. <https://doi.org/10.1.1.27.4399>.
- Setiawan, A. (2017). Enkripsi Citra Digital Menggunakan Metode Kurva Eliptik Diffie-Hellman dan Transformasi Wavlet Diskrit. *Departemen Matematika*.
- Singh, L. D., & Singh, K. M. (2015a). Image Encryption using Elliptic Curve Cryptography. *Procedia - Procedia Computer Science*, 54, 472–481. <https://doi.org/10.1016/j.procs.2015.06.054>.
- Singh, L. D., & Singh, K. M. (2015b). Image Encryption using Elliptic Curve Cryptography. *Procedia Computer Science*, 54, 472–481. <https://doi.org/10.1016/j.procs.2015.06.054>.
- Singh, L. D., & Singh, K. M. (2017). Medical image encryption based on improved Elgmal encryption. *Optik - International Journal for Light and Electron Optics*. <https://doi.org/10.1016/j.ijleo.2017.08.028>.
- Society, A. M. (2012). *Elliptic Curve Cryptosystems*. 48(177), 203–209. <https://doi.org/10.1007/978-3-642-04101-3>.
- Vigila, S. M. C., & Muneeswaran, K. (2009). Implementation of Text based Cryptosystem using Elliptic Curve Cryptography. *2009 1st International Conference on Advanced Computing, ICAC 2009*, <https://doi.org/10.1109/ICADVC.2009.5378025>.

